

FIG 1 – PRIOR ART

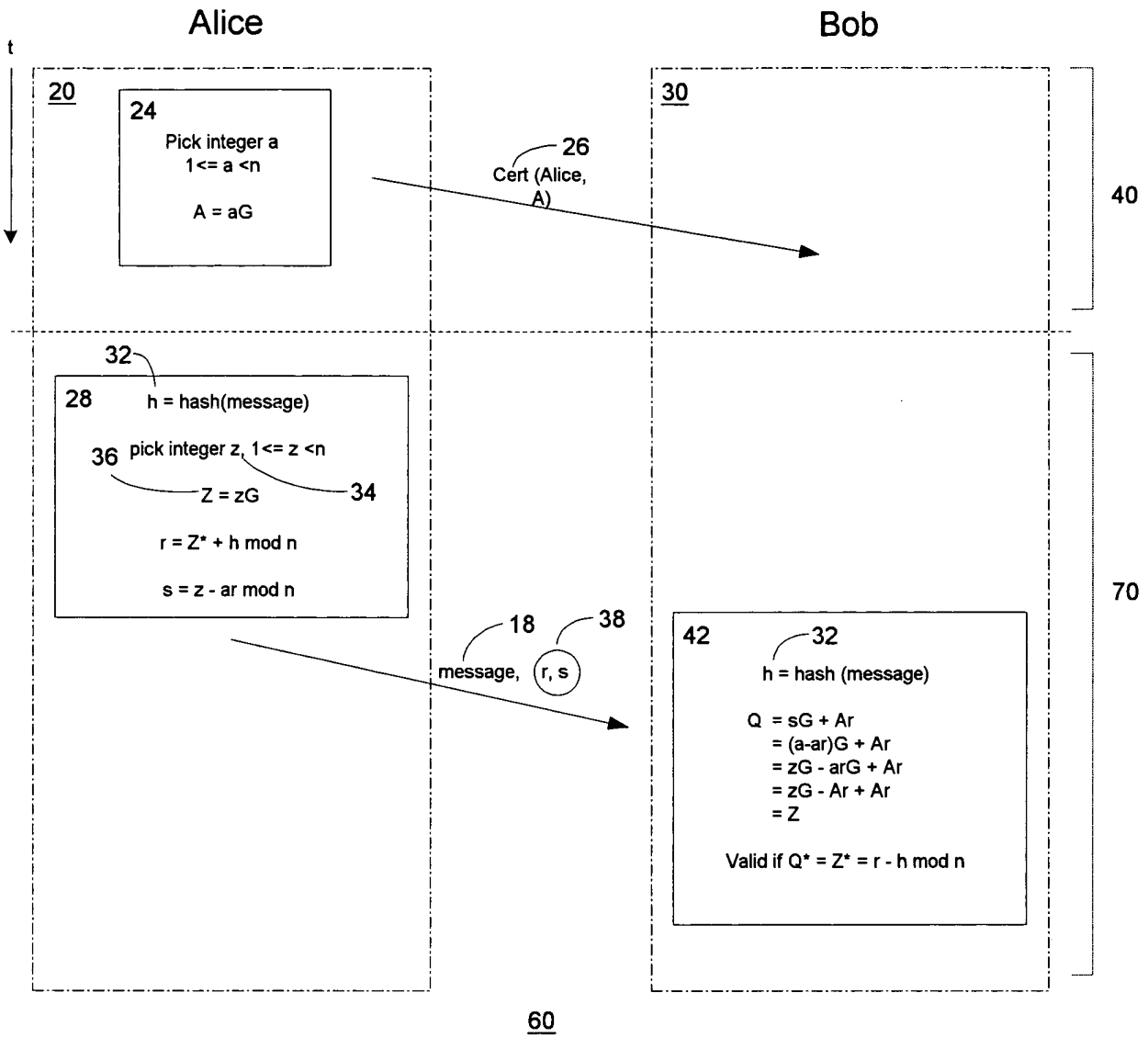


FIG. 2 – PRIOR ART

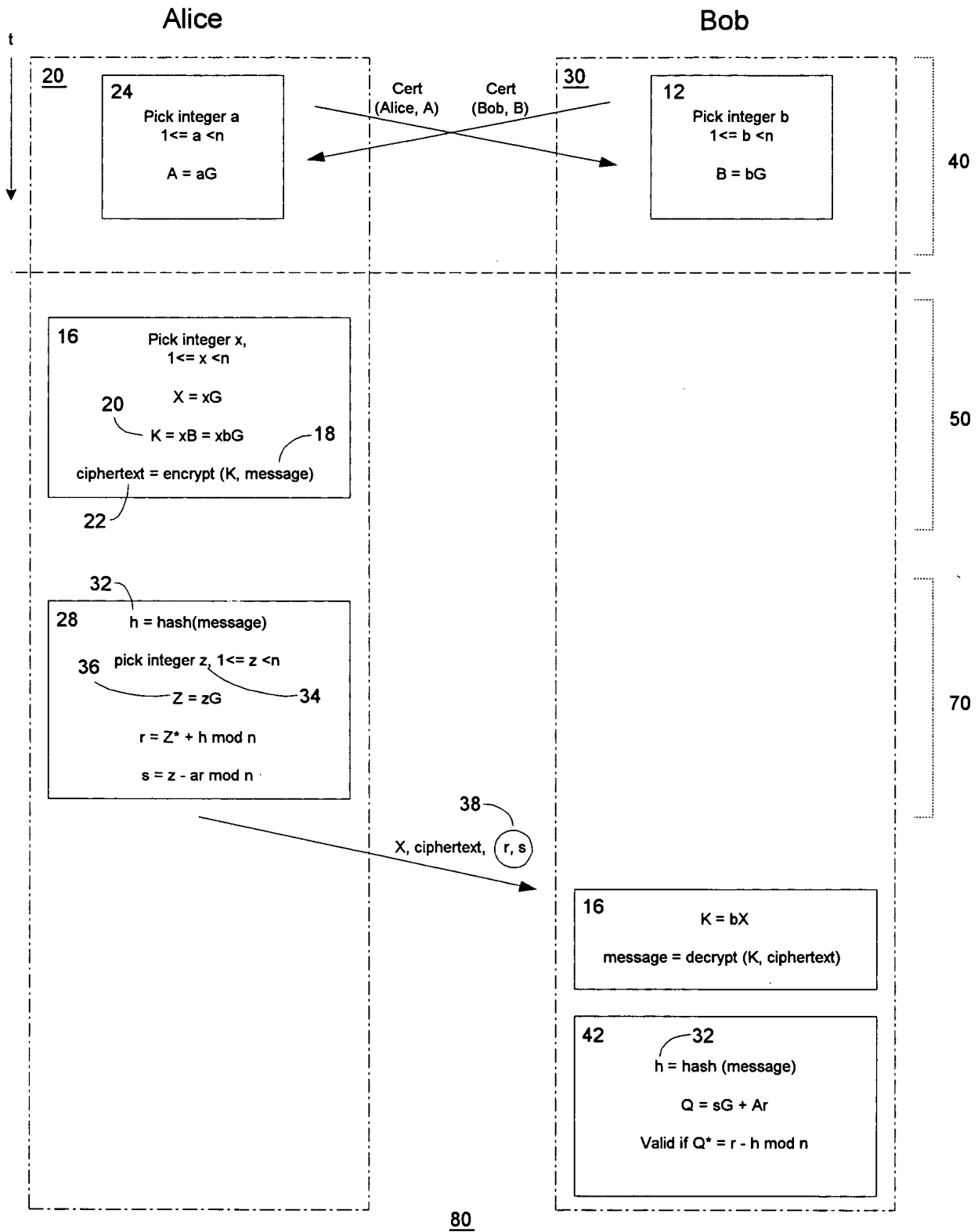


FIG. 1 is a flowchart illustrating a cryptographic process. The process starts with Alice (20) and Bob (30) exchanging certificates (Cert (Alice, A) and Cert (Bob, B)). Alice (24) picks an integer  $a$  such that  $1 \leq a < n$  and calculates  $A = aG$ . Bob (12) picks an integer  $b$  such that  $1 \leq b < n$  and calculates  $B = bG$ . Alice (16) picks an integer  $x$  such that  $1 \leq x < n$  and calculates  $X = xG$ . Alice (18) calculates  $K = xB = xbG$ . Alice (22) calculates ciphertext = encrypt ( $K$ , message). Alice (32) calculates  $h = \text{hash}(\text{message})$ . Alice (28) picks an integer  $z$  such that  $1 \leq z < n$  and calculates  $Z = zG$  (34). Alice calculates  $r = Z^* + h \bmod n$  and  $s = z - ar \bmod n$ . Alice (38) sends  $(X, \text{ciphertext}, r, s)$  to Bob. Bob (16) calculates  $K = bX$  and calculates message = decrypt ( $K$ , ciphertext). Bob (42) calculates  $h = \text{hash}(\text{message})$  (32) and calculates  $Q = sG + Ar$ . Bob checks if  $Q^* = r - h \bmod n$ .

FIG. 3 – PRIOR ART

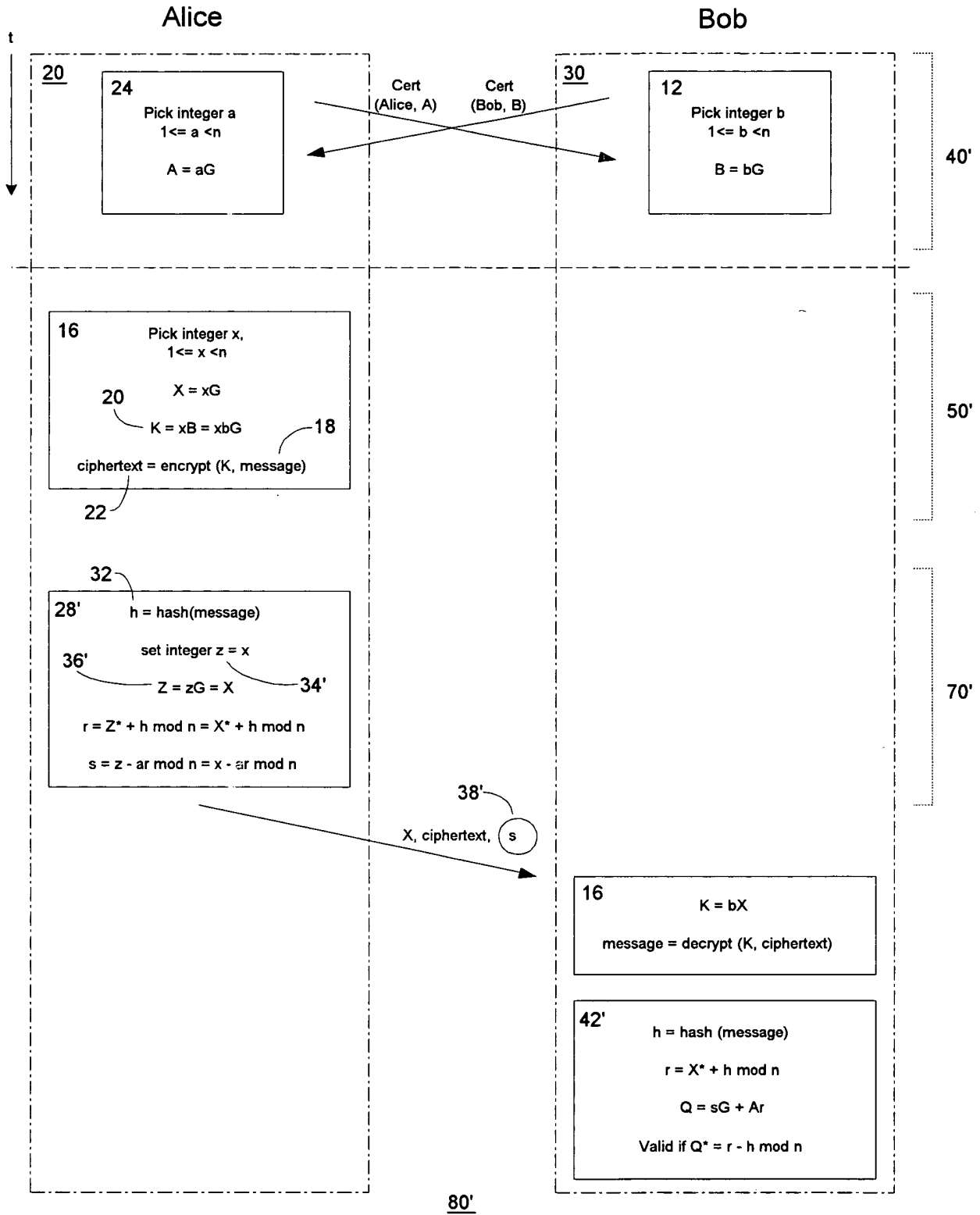


FIG. 4 - PRIOR ART

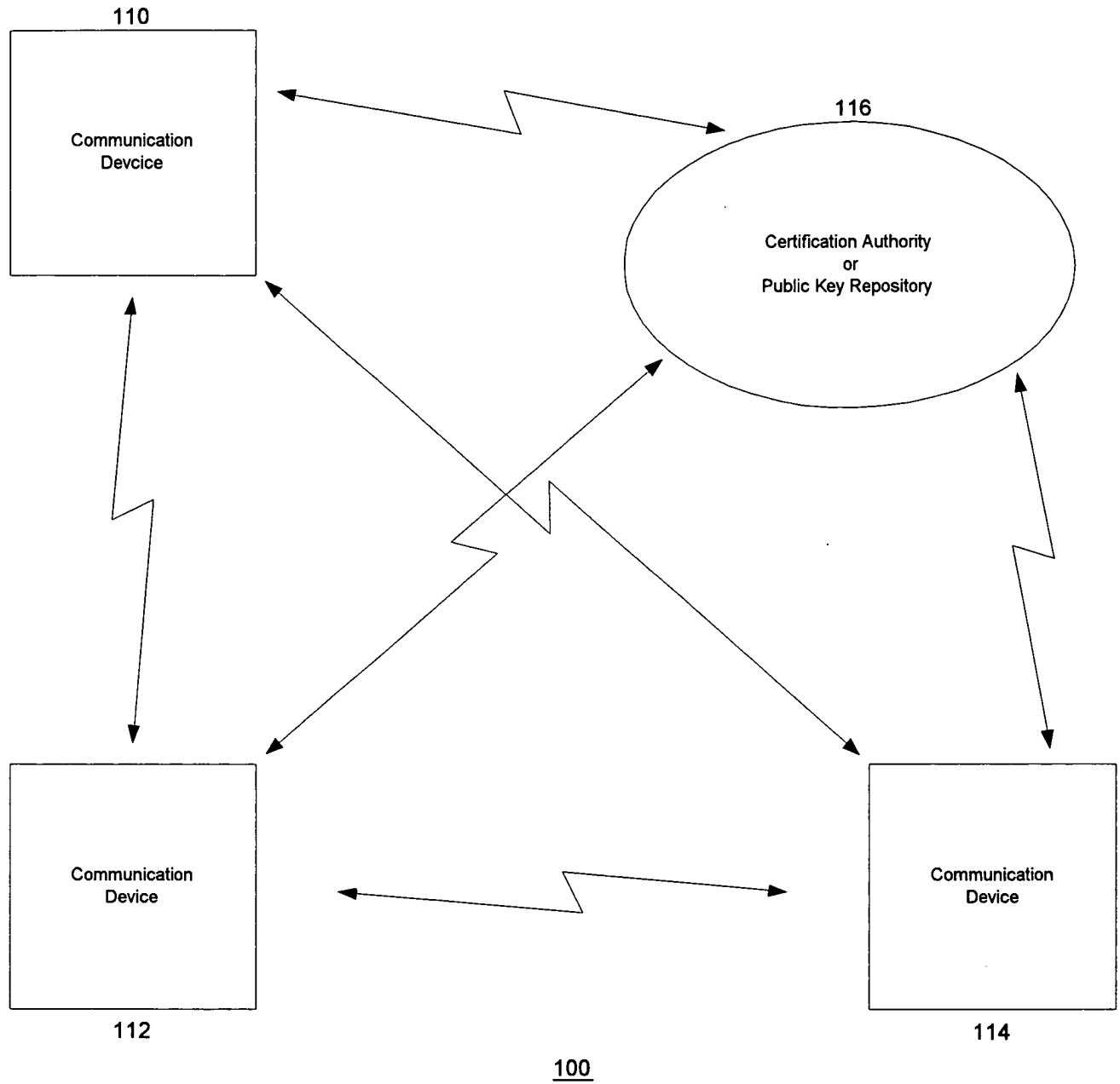


FIG. 5